(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
20. Oktober 2005 (20.10.2005)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2005/098567 A1

(51) Internationale Patentklassifikation[7]: G06F 1/00

(21) Internationales Aktenzeichen: PCT/EP2005/051072

(22) Internationales Anmeldedatum:
10. März 2005 (10.03.2005)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2004 014 435.4 24. März 2004 (24.03.2004) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **LINDINGER, Andreas** [DE/DE]; Im Winkel 12, 78658 Flözlingen (DE). **ROMBACH, Gerhard** [DE/DE]; Eichendorffweg 21, 78098 Triberg (DE). **LANGE, Roland** [DE/DE]; Goethestrasse 7, 78086 Brigachtal (DE). **KIEMES, Jochen** [DE/DE]; Mönsheimer Weg 14, 70499 Stuttgart (DE). **ASPERGER, Karl** [AT/AT]; Gassergasse 19, A-1050 Wien (AT).

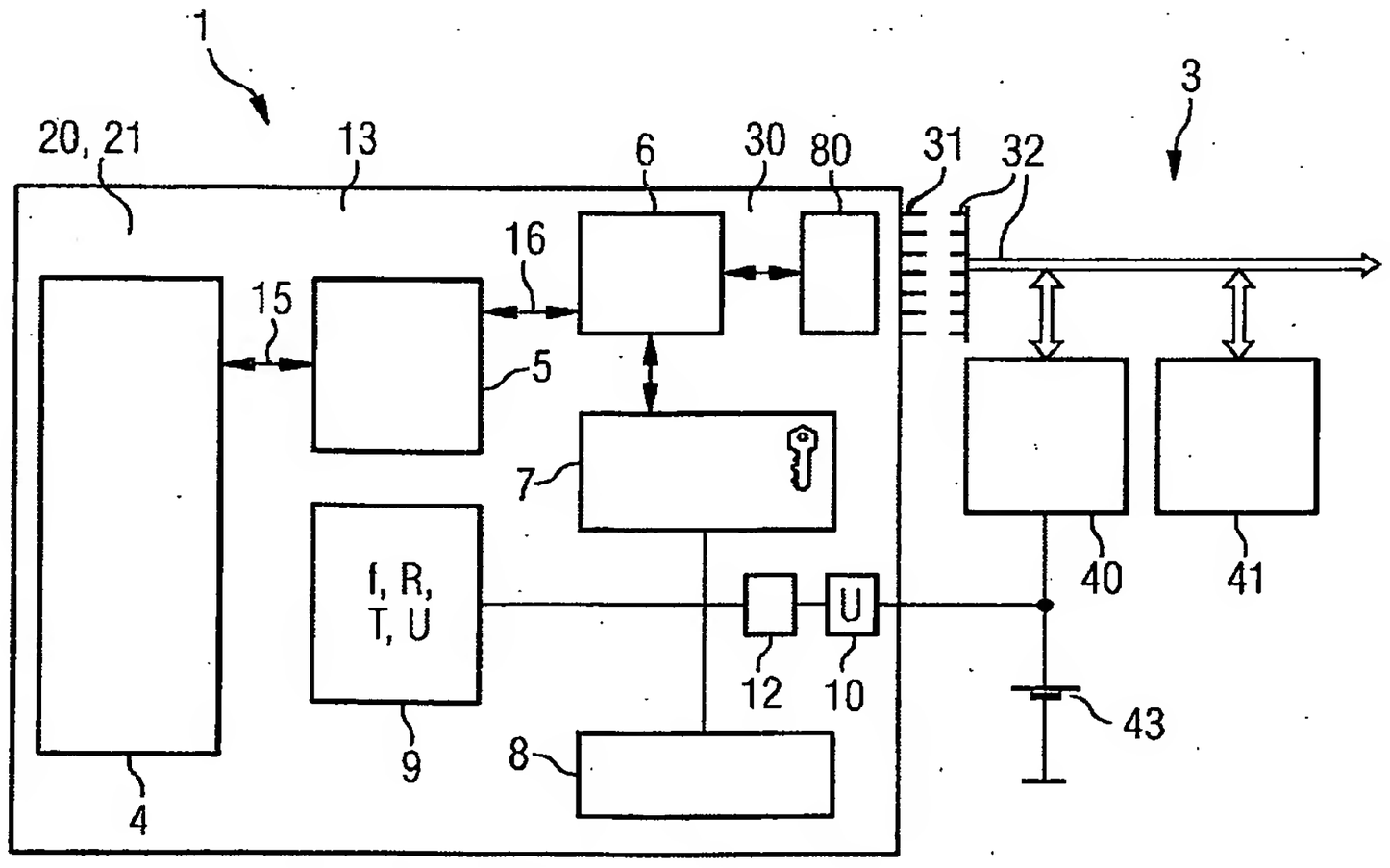
(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Postfach 22 16 34, 80506 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,

[Fortsetzung auf der nächsten Seite]

(54) **Title:** INTEGRATED CIRCUIT DEVICE

(54) **Bezeichnung:** ANORDNUNG MIT EINEM INTEGRIERTEN SCHALTKREIS



(57) **Abstract:** The invention relates to an integrated circuit (1) provided with function modules (2) which comprise a central processing unit (4) for treating data and executing a program and a cache memory (5). Until now, it was complicated and costly to ensure the manipulation security of said modules. Said invention makes it possible to take remedy actions.consisting in that the function modules (2) comprise an encoding unit (6) for data encoding and decoding.

[Fortsetzung auf der nächsten Seite]

WO 2005/098567 A1

KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Bestimmungsstaaten** *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:
— *mit internationalem Recherchenbericht*
— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) **Zusammenfassung:** Die Erfindung betrifft einen Integrierten Schaltkreis (1) mit Funktionsmodulen (2), wobei die Funktionsmodule (2) eine zentrale Verarbeitungseinheit (4), mittels welcher Daten verarbeitbar und Programme ausführbar sind, und einen Cachespeicher (5) umfassen. Die Gewährleistung einer Manipulationssicherheit derartiger Module ist bislang sehr aufwendig und geht mit hohen Kosten einher. Hier schafft die Erfindung Abhilfe, indem die Funktionsmodule (2) eine Verschlüsselungseinheit (6) umfassen, mittels welcher Daten verschlüsselbar und entschlüsselbar sind.

Beschreibung

Anordnung mit einem integrierten Schaltkreis

Die Erfindung betrifft eine Anordnung mit einem integrierten Schaltkreis und einen integrierten Schaltkreis mit Funktionsmodulen, wobei die Funktionsmodule eine zentrale Verarbeitungseinheit, mittels welcher Daten verarbeitbar und Programme ausführbar sind, und einen Cachespeicher umfassen.

Anordnungen mit integrierten Schaltkreisen der vorbeschriebenen Art finden sich heutzutage nahezu in sämtlichen Gebrauchsgegenständen mit integrierter Elektronik. Geräte zur elektronischen Datenverarbeitung, Kommunikation oder zur Aufzeichnung von Daten weisen, je nach Art der behandelten Daten, Vorkehrungen auf, die den Lese-, Schreib- oder Änderungszugriff auf die Daten einschränken. Hierdurch sollen Daten vor öffentlicher Zugänglichkeit oder Manipulation geschützt werden. Insbesondere im Bereich der zukünftigen Fahrtschreibergeneration, dem digitalen Tachografen, ist ein Schutz der aufgezeichneten Daten gegen eine Manipulation von höchster Bedeutung.

Bisherige manipulationssichere Systeme mit hohen Sicherheitsanforderungen bestehen regelmäßig aus mehreren diskreten Baugruppen, denen unterschiedliche Funktionen zugeordnet sind, beispielsweise sind eine zentrale Verarbeitungseinheit, eine Verschlüsselungseinheit und verschiedene Speicher jeweils regelmäßig eine eigenständige Einheit, die mit den übrigen Einheiten in Verbindung steht. Das Erfordernis mehrerer Baugruppen und deren Zusammenstellung sowie Abstimmung aufeinander geht mit hohen Kosten in der Serienproduktion einher.

Ausgehend von den Problemen und Nachteilen des Standes der Technik liegt der Erfindung die Aufgabe zugrunde, eine Anordnung der eingangs genannten Art zu schaffen, welche höchsten Anforderungen der Manipulationssicherheit genügt und gleichzeitig eine Eignung für die Serienproduktion bei geringeren Kosten aufweist.

Die erfindungsgemäße Aufgabe wird mittels eines integrierten Schaltkreises der eingangs genannten Art gelöst, welcher eine Verschlüsselungseinheit als Funktionsmodul umfasst, mittels derer Daten oder Programmcode verschlüsselbar und entschlüsselbar sind.

Dadurch, dass eine Verschlüsselungseinheit als Funktionsmodul des integrierten Schaltkreises Element dieses Bauteiles ist, kann in der Fertigung und Entwicklung einer Anordnung mit einem erfindungsgemäßen integrierten Schaltkreis die zusätzliche Bereitstellung, Montage und Abstimmung auf umliegende Bauelemente eingespart werden. In synergetischer Weise ergibt sich der weitere große Vorteil, dass die Verschlüsselungseinheit von dem integrierten Schaltkreis, dessen Bestandteil sie ist, nur schwer zu trennen ist und daher Versuche der Manipulation zum Scheitern verurteilt sind.

Die Manipulation eines erfindungsgemäßen integrierten Schaltkreises, insbesondere die Abtrennung einzelner Funktionsmodule, gestaltet sich besonders schwierig, wenn der integrierte Schaltkreis als Halbleiterchip ausgebildet ist, insbesondere, wenn einzelne Funktionsmodule puzzleartig ineinander greifen, in einer Weise, dass einzelne Funktionsmodule diskret nicht mehr erkennbar sind. Hier können besonders komplexe geometrische Verstrickungen gewählt werden, so dass die miteinander vermischten Halbleiterstrukturen sich mittels einer Analyse

in Manipulationsabsicht nicht mehr als solche trennbar erkennen lassen.

Zusätzliche Sicherheit gegen Manipulation wird gewonnen, wenn die Funktionsmodule einen ersten Speicher umfassen, in welchem kryptologische Schlüssel abgespeichert sind. Die Integration eines solchen ersten Speichers erschwert einen gezielten Zugriff und ein gezieltes Auslesen der kryptologischen Schlüssel.

Der Aufwand für eine Verwaltung kryptologischer Schlüssel durch den Hersteller der Geräte entfällt vollständig bei zusätzlichem Sicherheitsgewinn, wenn die Funktionsmodule einen Zufallszahlengenerator (RNG) umfassen, der die kryptologischen Schlüssel gleichsam autonom erzeugt. Diese Schlüssel können zweckmäßig in dem ersten Speicher abgelegt werden.

Mit Vorteil kann als weiteres Funktionsmodul eine Real-Time-Clock in den integrierten Schaltkreis eingegliedert werden, deren korrekte Funktion ebenfalls hohe Relevanz für die Sicherheit gegen Manipulation hat.

Damit der Manipulationsangriff nicht nur erschwert, sondern unmöglich gemacht wird, kann mit Vorteil eine Sicherheitssensorik in dem Schaltkreis als Funktionsmodul integriert werden, mittels derer mindestens ein Betriebsparameter des integrierten Schaltkreises überwachbar ist. Geeignete Betriebsparameter für die Überwachung sind beispielsweise die Taktfrequenz der Real-Time-Clock, der System- bzw. CPU-Takt, oder eine Betriebstemperatur, oder eine Betriebsspannung des integrierten Schaltkreises, oder der Zustand einer Schutzschicht auf dem integrierten Schaltkreis, oder eine Kombination der vorgenannten Betriebsparameter. Ist der integrierte

Schaltkreis als Halbleiterbauelement ausgebildet, so ist die Überwachung des Zustandes einer Schutzschicht auf dem integrierten Schaltkreis besonders effektiv, da die Schutzschicht zerstört werden muss, um mechanisch auf der Struktur des Halbleiterchips zuzugreifen. Hierbei ist es zweckmäßig, wenn die Schutzschicht als aktive Schutzschicht ausgebildet und direkt auf dem Die des Halbleiterchips aufgebracht ist. Eine zweckmäßige Weiterbildung sieht vor, dass die aktive Schutzschicht aus mindestens einer länglichen elektrischen Leitung besteht, welche entlang der Oberfläche des Dies, insbesondere abschnittsweise in untereinander parallelen Bahnen verläuft. Die Überwachung kann beispielsweise eine Überwachung des ohmschen Widerstands der elektrischen Leitung sein, wobei zweckmäßig eine Änderung des Widerstandswertes, die auf eine Zerstörung der elektrischen Leitung schließen lässt, eine Löschung der zu schützenden Daten bewirkt. Vorzugsweise wird der Mikrocontroller in einen gesicherten Zustand, beispielsweise Reset, überführt. Auf diese Weise wird das System "integrierter Schaltkreis" nach der Erfindung vergleichsweise eigensicher.

Zweckmäßig gestaltet sich die Überwachung des Betriebsparameters in der Weise, dass mindestens ein Grenzwert für den zu überwachenden Betriebsparameter vorgegeben ist, der Betriebsparameter gemessen und mit dem Grenzwert verglichen wird und bei einem Überschreiten oder Unterschreiten des Grenzwertes der Inhalt des ersten Speichers gelöscht wird. Zweckmäßig ist der Grenzwert so zu wählen, dass die Vorgaben des Normalbetriebs nicht zu einer Funktionsunterbrechung der Anordnung führen, beispielsweise im Automotive-Bereich bei einer Temperatur von -40 °C noch keine Löschung der Daten erfolgt.

Die Handhabbarkeit und Sicherheit des erfindungsgemäßen integrierten Schaltkreises erhöht sich zusätzlich, wenn er in einem Gehäuse angeordnet ist und aus dem Gehäuse herausgeführte Anschlusskontakte aufweist. Zum Zweck einer mechanischen Manipulation müsste demgemäß zunächst das Gehäuse geöffnet werden.

Eine höhere Integration des erfindungsgemäßen Schaltkreises kann erreicht werden, wenn einzelne Funktionsmodule eine im Wesentlichen flächige Erstreckung aufweisen und in Richtung der Flächennormalen benachbart zueinander angeordnet sind. So kann zum Beispiel die zentrale Verarbeitungseinheit gestapelt mit verschiedenen Speichern oder anderen Funktionsmodulen angeordnet werden.

Mit Vorteil können Angriffe, die Rückschlüsse auf den Funktionszustand aus dem Verhalten des Versorgungsstromes des integrierten Schaltkreises schließen, abgewehrt werden, wenn die Funktionsmodule einen integrierten Spannungsregler umfassen, der die Betriebsspannung regelt und auf diese Weise nach außen hin diesen Betriebsparameter vergleichsweise verrauscht.

Besondere Vorteile entfaltet der erfindungsgemäße integrierte Schaltkreis in einer Anordnung mit einem zweiten Speicher, der mittels eines Datenbusses mit dem erfindungsgemäßen integrierten Schaltkreis in Verbindung steht, in welchem zweiten Speicher Daten oder Programmcode verschlüsselt abgelegt sind und der Speicherzellen aufweist, welche jeweils eine Speicheradresse aufweisen und jede Speicherzelle direkt lesend oder schreibend angesprochen werden kann. Um die gesamte Anordnung gegenüber dem Ausfall einer externen Spannungsversorgung abzusichern, ist es zweckmäßig, wenn sie mit einer

Batterie in Verbindung steht, so dass die Spannungsversorgung bei einem Fehlen anderer Energieversorgung aufrechterhaltend ist. Insofern lassen sich auch Kosten einsparen, wenn der zweite Speicher kostengünstig flüchtig ausgebildet und mittels der Batterie abgepuffert ist.

Ersatzweise oder in Ergänzung zu dem zweiten Speicher kann ein dritter Speicher zweckmäßig sein, der mit dem integrierten Schaltkreis mittels eines Datenbusses in Verbindung steht und nicht flüchtig ausgebildet ist, insbesondere als Flash oder ROM ausgebildet ist, wobei in dem dritten Speicher die Daten oder Programmcode vorzugsweise verschlüsselt abgelegt sind.

Besonders vorteilhaft ist eine Abpufferung der Sicherheitssensorik mittels einer Batterie. Alternativ oder in Ergänzung zu dieser Maßnahme kann eine in dem Gehäuse integrierte Hilfsenergiequelle, beispielsweise ein Kondensator, vorgesehen sein, welcher die Energie im Falle eines registrierten Manipulationsversuches zum Löschen der Speicher, insbesondere des ersten Speichers, bereitstellt.

Im Folgenden ist die Erfindung anhand eines speziellen Ausführungsbeispiels zur Verdeutlichung näher beschrieben. Neben diesem Ausführungsbeispiel ergeben sich für den Fachmann aus der hier beschriebenen Erfindung zahlreiche andere Möglichkeiten der Gestaltung. Insbesondere sind der Erfindung auch Merkmalskombinationen zuzurechnen, welche sich aus Kombinationen der Ansprüche ergeben, auch wenn kein ausdrücklicher dementsprechender Rückbezug angeführt ist. Es zeigen:

Figur 1 eine schematische Darstellung einer erfindungsgemäßen Anordnung.

Figur 1 zeigt einen integrierten Schaltkreis 1 mit verschiedenen Funktionsmodulen 2, der mit externen Bauelementen 3 in Verbindung steht. Der integrierte Schaltkreis weist neben einer zentralen Verarbeitungseinheit 4 noch weitere Funktionsmodule 2 auf, nämlich einen Cachespeicher 5, eine Verschlüsselungseinheit 6, einen ersten Speicher 7, eine Real-Time-Clock 8, einen Zufallszahlengenerator 80 und eine Sicherheitssensorik 9. Daneben sind ein Spannungsregler 10 und eine Hilfsenergiequelle 12 integrierte Bauelemente des als Halbleiterchip 13 ausgebildeten integrierten Schaltkreises 1. Die zentrale Verarbeitungseinheit 4 verarbeitet Daten oder führt Programme aus, welche sie mittels eines ersten Datenbusses 15 aus dem Cachespeicher 5 ausliest.

Der Cachespeicher 5 steht mit der Verschlüsselungseinheit 6 mittels eines zweiten Datenbusses 16 in Verbindung. Die Verschlüsselungseinheit 6 liest aus dem zweiten oder dritten Speicher 40, 41 mittels des Adress-Datenbusses 32 die verschlüsselten Daten bzw. Code ein, entschlüsselt sie mittels des im ersten Speicher 7 abgelegten kryptografischen Schlüssels 18 und schreibt sie in den Cache bzw. in andere interne Register der zentralen Verarbeitungseinheit 4. Die kryptologischen Schlüssel 18 sind zuvor von dem Zufallszahlengenerator 80 erzeugt worden. Der Zufallszahlengenerator 80 verwendet zur Erzeugung der kryptografischen Schlüssel 18, welche im ersten Speicher 7 abgelegt sind beispielsweise die Startwerte aus den statistischen Schwankungen (Rauschen) von internen, physikalischen Messgrößen, wie Chiptemperatur, Versorgungsspannung, Taktfrequenz.

Die Sicherheitssensorik 9 überwacht neben der Betriebstemperatur T, der Betriebsspannung U, der Taktfrequenz f auch den ohmschen Widerstand R einer Schutzschicht 20, welche aus zu-

einander im Wesentlichen parallelen Bahnen einer elektrischen Leitung 21 besteht, die direkt auf dem Die des Halbleiterchips 13 aufgebracht sind. Der gemessene Widerstand R wird permanent mit einem Grenzwert verglichen, und bei Überschreitung des Grenzwertes veranlasst die zentrale Verarbeitungseinheit 4 die Löschung des ersten Speichers 7, wobei der integrierte Schaltkreis 1 anschließend in einen gesicherten Zustand, beispielsweise Reset, überführt wird.

Der integrierte Schaltkreis 1 ist von einem Gehäuse 30 umgeben, welches Anschlusskontakte 31 aufweist, die zumindest teilweise mit einem Adress-Datenbus 32 in Verbindung stehen. Mittels des Adress-Datenbusses 32 tauscht der integrierte Schaltkreis 1 Daten mit einem zweiten Speicher 40 und einem dritten Speicher 41 aus. Der zweite Speicher 40 ist als flüchtiges RAM ausgebildet und mittels einer Batterie 43 gegen Spannungsausfall ebenso wie der integrierte Schaltkreis 1 abgesichert. Der dritte Speicher 41 ist nicht flüchtig als Flash oder ROM ausgebildet. Die in dem zweiten Speicher 40 und dritten Speicher 41 abgelegten Daten sind unter Verwendung der kryptologischen Schlüssel 18 verschlüsselt und werden bei jedem Zugriff mittels der Verschlüsselungseinheit 6 verschlüsselt oder entschlüsselt.

Patentansprüche

1. Integrierter Schaltkreis (1) mit Funktionsmodulen (2), wobei die Funktionsmodule (2) eine zentrale Verarbeitungseinheit (4), mittels welcher Daten verarbeitbar und Programme ausführbar sind, und einen Cachespeicher (5) umfassen, dadurch gekennzeichnet, dass die Funktionsmodule (2) eine Verschlüsselungseinheit (6) umfassen, mittels welcher Daten verschlüsselbar und entschlüsselbar sind.

2. Integrierter Schaltkreis (1) nach Anspruch 1, dadurch gekennzeichnet, dass die Funktionsmodule einen Zufallszahlengenerator (80) umfassen.

3. Integrierter Schaltkreis (1) nach Anspruch 1, dadurch gekennzeichnet, dass die Funktionsmodule (2) einen ersten Speicher (7) umfassen, in welchem kryptologische Schlüssel (18) abgespeichert sind.

4. Integrierter Schaltkreis (1) nach Anspruch 2 und 3, dadurch gekennzeichnet, dass krypotologische Schlüssel (18), welche in dem ersten Speicher (7) abgespeichert sind, mittels des Zufallszahlengenerators (80) erzeugt sind.

5. Integrierter Schaltkreis (1) nach Anspruch 1, dadurch gekennzeichnet, dass die Funktionsmodule (2) eine Real-Time-Clock (8) umfassen.

6. Integrierter Schaltkreis (1) nach Anspruch 1, dadurch gekennzeichnet, dass die Funkti-

onsmodule (2) eine Sicherheitssensorik (9), mittels derer mindestens ein Betriebsparameter (f, T, U) des integrierten Schaltkreises (1) überwachbar ist, umfassen.

7. Integrierter Schaltkreis (1) nach Anspruch 6, dadurch gekennzeichnet, dass der Betriebsparameter (f, T, U) die Taktfrequenz (f) der Real-Time-Clock (8) und/oder eine Betriebstemperatur (T) an einer Stelle des Integrierten Schaltkreises (1) und/oder eine Betriebsspannung (U) des integrierten Schaltkreises (1) und/oder der Zustand einer Schutzschicht (20) auf dem Integrierten Schaltkreis (1) ist.

8. Integrierter Schaltkreis (1) nach Anspruch 6, dadurch gekennzeichnet, dass für den zu überwachenden Betriebsparameter (f, T, U) mindestens ein Grenzwert vorgegeben ist, der Betriebsparameter (f, T, U) gemessen wird und mit dem Grenzwert verglichen wird und bei einem Überschreiten oder Unterschreiten des Grenzwertes der Inhalt des ersten Speichers gelöscht wird.

9. Integrierter Schaltkreis (1) nach Anspruch 1, dadurch gekennzeichnet, dass er in einem Gehäuse (30) angeordnet ist und aus dem Gehäuse (30) herausgeführte Anschlusskontakte (31) aufweist.

10. Integrierter Schaltkreis (1) nach Anspruch 1, dadurch gekennzeichnet, dass einzelne Funktionsmodule (2) eine im Wesentlichen flächige Erstreckung aufweisen und in Richtung der Flächennormalen benachbart zueinander angeordnet sind.

11. Integrierter Schaltkreis (1) nach Anspruch 1, dadurch gekennzeichnet, dass die Funktionsmodule (2) einen integrierten Spannungsregler umfassen, welcher eine Betriebsspannung (U) regelt.

12. Integrierter Schaltkreis (1) nach Anspruch 1, dadurch gekennzeichnet, dass er als Halbleiterchip (13) ausgebildet ist.

13. Integrierter Schaltkreis (1) nach Anspruch 12, dadurch gekennzeichnet, dass Halbleiterstrukturen der einzelnen Funktionsmodule (2) puzzleartig ineinander greifen, zur Vermeidung, dass einzelne Funktionsmodule (2) erkennbar sind.

14. Integrierter Schaltkreis (1) nach Anspruch 12, dadurch gekennzeichnet, dass direkt auf dem Die des Halbleiterchips (13) eine aktive Schutzschicht (20) aufgebracht ist, welche aus mindestens einer länglichen elektrischen Leitung (21) besteht, welche entlang der Oberfläche des Dies, insbesondere abschnittsweise in zueinander parallelen Bahnen verläuft.

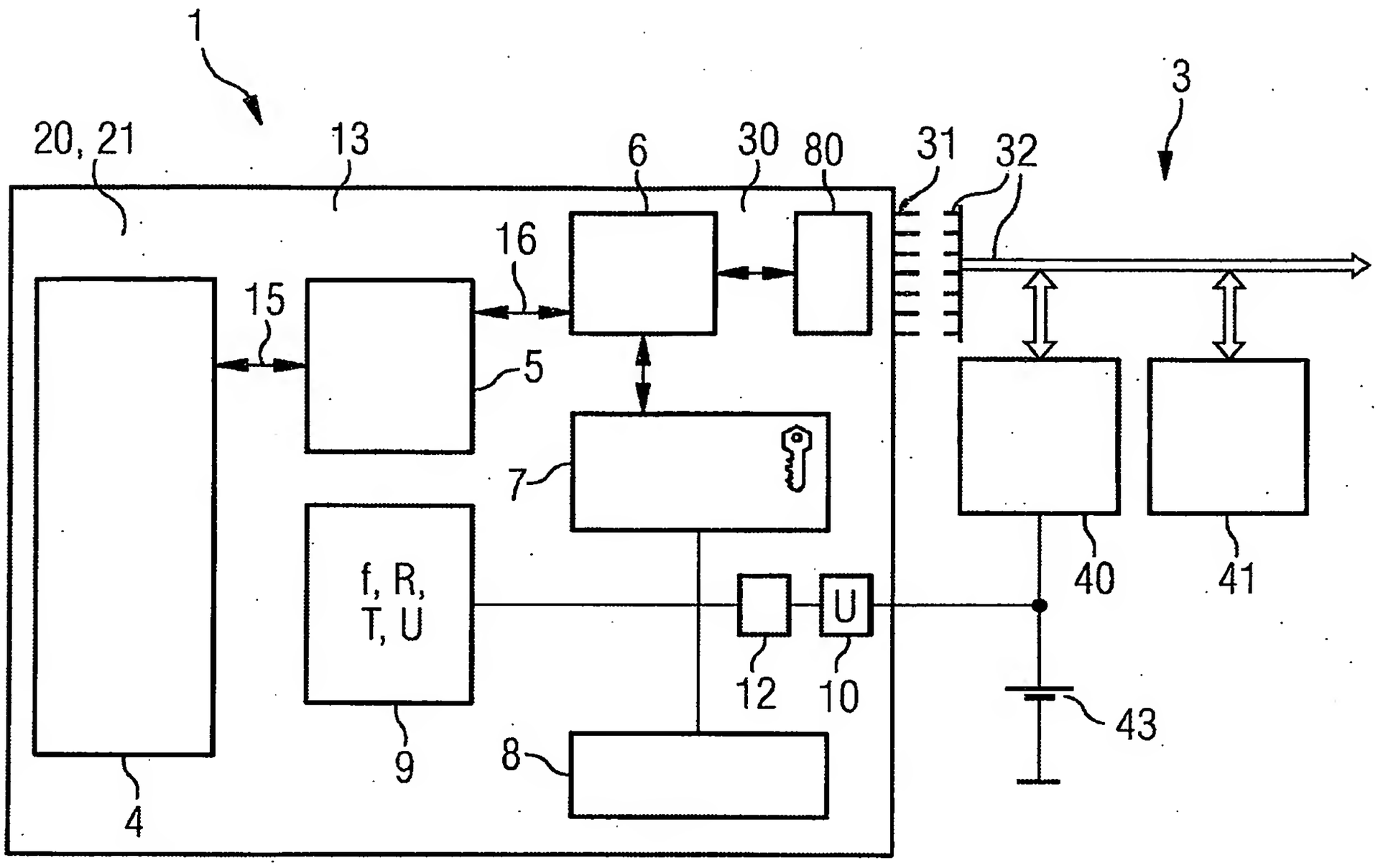
15. Anordnung mit einem integrierten Schaltkreis (1) nach einem der Anspruche 1 bis 14, dadurch gekennzeichnet, dass der integrierte Schaltkreis (1) mittels eines Datenbusses (32) mit einem zweiten Speicher (40) [RAM] in Verbindung steht, in welchem Daten verschlüsselt abgelegt sind, wobei der zweite Speicher (40) Speicherzellen aufweist, welche jeweils eine Speicheradresse aufweisen und jede Speicherzelle direkt lesend oder schreibend angesprochen werden kann.

16. Anordnung mit einem integrierten Schaltkreis (1) nach einem der Anspruche 1 bis 14, dadurch gekennzeichnet, dass der zweite Speicher (40) flüchtig ist und mit einer Batterie (43) in Verbindung steht, so dass die Spannungsversorgung bei einem Fehlen anderer Energieversorgung aufrechterhalten ist.

17. Anordnung mit einem integrierten Schaltkreis (1) nach einem der Anspruche 1 bis 14, dadurch gekennzeichnet, dass der integrierte Schaltkreis (1) mittels eines Datenbusses (32) mit einem nichtflüchtigen dritten Speicher (41), insbesondere einem Flash oder ROM in Verbindung steht, in welchem Daten oder Programmcode verschlüsselt abgelegt sind.

18. Anordnung mit einem integrierten Schaltkreis (1) nach Anspruch 6, dadurch gekennzeichnet, dass die Sicherheitssensorik (9) mit einer Batterie (43) in Verbindung steht, so dass die Spannungsversorgung bei einem Fehlen anderer Energieversorgung aufrechterhalten ist.

19. Anordnung mit einem integrierten Schaltkreis (1) nach Anspruch 6, dadurch gekennzeichnet, dass die Sicherheitssensorik (9) mit einer in dem Gehäuse (30) integrierten Hilfsenergiequelle (12) in Verbindung steht, welche die Energie zum Löschen ersten Speichers (7) bereitstellt.


1
20, 21
13
6
30
80
31
32
3
16
15
5
7
f, R,
T, U
12
U
10
40
41
43
9
8
4

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2005/051072

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 943 421 A (GRABON ET AL) 24 August 1999 (1999-08-24)	1
Y	abstract; figures 1,2 column 1, line 10 - line 25 column 4, line 23 - column 6, line 63 column 3, line 25 - line 45	2-4
X	US 6 523 118 B1 (BUER MARK LEONARD) 18 February 2003 (2003-02-18)	1
Y	abstract; figure 1 column 1, line 10 - line 38 column 3, line 9 - line 14 column 3, line 1 - column 4, line 6	2-4
Y	US 5 473 692 A (DAVIS ET AL) 5 December 1995 (1995-12-05) abstract; figure 5 column 6, line 37 - line 61 column 7, line 38 - line 42	2-4

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 June 2005	18. 08. 2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Harms, C

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2005/051072

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

See additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-4

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2005/051072

Continuation of Box III

The International Searching Authority has found that the international application contains multiple (groups of) inventions, as follows:

1. Claims 1-4

   Integrated circuit with central processor unit, cache memory and encryption unit; generation of the cryptographic keys by a random number generator in the integrated circuit.

2. Claim 5

   Integrated circuit with central processor unit, cache memory and encryption unit; real-time clock.

3. Claims 6-8

   Integrated circuit with central processor unit, cache memory and encryption unit; security sensor system for monitoring the operating parameters of the integrated circuit.

4. Claim 9

   Integrated circuit with central processor unit, cache memory and encryption unit; housing and terminal contacts.

5. Claim 10

   Integrated circuit with central processor unit, cache memory and encryption unit; spatial arrangement of the function modules.

6. Claim 11

   Integrated circuit with central processor unit, cache memory and encryption unit; integrated voltage regulator for controlling the operating voltage.

7. Claims 12-14

   Integrated circuit with central processor unit, cache memory and encryption unit; integrated circuit in the form of a semiconductor chip.

8. Claim 15

Integrated circuit with central processor unit, cache memory and encryption unit; encryption of the contents of the connected RAM.

9. Claim 16

Integrated circuit with central processor unit, cache memory and encryption unit; connected RAM powered by a battery.

10. Claim 17

Integrated circuit with central processor unit, cache memory and encryption unit; encryption of program code in a non-volatile third memory.

11. Claims 18 and 19

Integrated circuit with central processor unit, cache memory and encryption unit; security sensor system powered by its own battery.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2005/051072

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5943421 A	24-08-1999	US 6538413 B1	25-03-2003
		US 5898290 A	27-04-1999
US 6523118 B1	18-02-2003	NONE	
US 5473692 A	05-12-1995	AU 3583295 A	27-03-1996
		EP 0780039 A1	25-06-1997
		JP 10507324 T	14-07-1998
		RU 2147790 C1	20-04-2000
		WO 9608092 A1	14-03-1996
		US 5568552 A	22-10-1996